UNITED STATES DISTRICT COURT

for the

District of Guam

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

Information Associated with davecabrera269@gmail.com, which is stored at premises controlled by Google, Inc. (Further described in Attachment A)

Case No. MJ- 18-00033

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

Information Associated with davecabrera269@gmail.com, which is stored at premises controlled by Google, Inc. Further described in Attachment A.

located in the _____ District of Guam, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B which is incorporated herein.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 USC § 371	Conspiracy
18 USC § 1343	Wire Fraud
18 USC §§ 1956(h) & 1957	Money Laundering

The application is based on these facts:

- ☑ Continued on the attached sheet.
- ☑ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

JOSHUA M. KIPP, Special Agent, FBI
Printed name and title

Sworn to before me and signed in my presence.

Date: 3/2/18

Judge's signature

City and state: Hagatna, Guam

JOAQUIN V.E. MANIBUSAN, JR., U.S. Magistrate Judge
Printed name and title

ORIGINAL

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

I, Joshua M. Kipp, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with certain accounts that are stored at premises controlled by Google, Inc., an email provider headquartered at Mountain View, California. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Google, Inc., to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

2. I am a duly appointed Special Agent of the FBI, and have been for over fourteen (14) years in various locations. I am currently assigned to work various violations, to include white collar crimes within the Honolulu Field Office, Guam Resident Agency. I have received training in connection with, and participated in, investigations involving various forms of fraud, including but not limited to criminal enterprises, fraudulent statements and/or entries, loan and credit applications fraud, wire fraud, government fraud, mortgage and bank fraud. I have experience in conducting criminal investigations of criminal groups and conspiracies, as well as the collection of evidence and the identification and use of witnesses.

3. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of Title 18, United States Code, Section 371 (Conspiracy) Title 18, United States Code, Section 1343 (Wire Fraud), Title 18, United States Code, Section 1956(h) and 1957 (Money Laundering) were committed. As set forth below, there is probable cause to believe the Target Email Accounts contain evidence of wire fraud committed by John Shen (Shen Sr.), aka Chi Jung Shen, Ana Absalon, and others yet unknown, in violation of Title 18, United States Code, Section 1343.

JURISDICTION

5. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by Title 18, United States Code, Section 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is "a district court of the United States ... that – has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

FACTS ESTABLISHING PROBABLE CAUSE

6. From approximately October 2013 to August 2015, Shen Sr. and Sales Administrator Ana Absalon used alias email accounts to facilitate a fraud scheme wherein sixty-one (61) vehicles were fraudulently registered to "end-customers" on Guam, by creating false documentation, when in fact Shen Sr. was selling the vehicles to an automobile broker(s) in China, netting gross sales of $5,575,309.75.

PROBABLE CAUSE

7. John C. J. Shen (Shen Sr.), also known as Chi-Jung Shen, is the owner or controls Shen's Corporation, Shen's Enterprises, MGT Corporation, and Pan Asia Wholesale Corporation. Shen's Corporation dba Prestige Automobiles operates a retail car sales business

located at 491 East Marine Corps Drive, Dededo, Guam. Prestige Automobiles was formed in 1991.

8. In February 1992, Shen Sr., as the President for Prestige Automobiles, signed a Bavarian Motor Works (BMW) Importer Contract in which Shen Sr. agreed that Prestige Automobiles territory to sell BMW vehicles was the island of Guam. Shen Sr. agreed that sales outside of Prestige Automobiles' contract territory, directly or indirectly, was prohibited, and that it was the full responsibility of Shen to ensure that vehicles are only being sold to "end-customers" and not to unauthorized resellers. Shen Sr. signed Contract Renewal Letters with BMW for 2013, 2014, and an updated Importer Contract in 2015, acknowledging and agreeing to abide by the above requirements.

9. On January 1, 2012, Shen Sr., as the President for Prestige Automobiles, signed a franchise agreement with Jaguar Land Rover North America, LLC (Land Rover). Attached with the franchise agreement was Land Rover's Standard Terms and Conditions which outlined Prestige Automobiles' office to be on Guam and sales territory to be the islands of Guam, Saipan, Rota and Tinian. In section 4.3 of the Standard Terms and Conditions it states that the Dealer, Prestige Automobiles, agrees to conduct operations from such facilities and none other.

10. From at least October 2013 through August 2015, Shen Sr., through his corporations, affiliated businesses and Prestige Automobiles, sold sixty-one (61) vehicles to an automobile broker(s) in China through a fraudulent scheme. The scheme included creating false documentation to make it appear that Shen Sr. was selling the vehicles to "end-customers" on Guam and not making sales to customers in China. Sales of the sixty-one (61) vehicles to China

netted Shen Sr. gross sales of $5,575,309.75 during the period of October 2013 through August 2015.

11. The fictitious sales were conducted through three (3) known fraud techniques. No sales purchase money was exchanged between the alleged Guam buyers and Prestige Automobiles. The techniques were as follows:

a. Shen Sr. and others employed the technique of identity theft to create fictitious local buyers to make it appear the car was sold to the victims of identity theft on Guam.

b. Shen Sr. and others recruited individuals on Guam who were paid by Shen Sr. for the use of their names and/or business entity names to be listed as buyers of vehicles (Straw buyers)

c. Shen Sr. and others created Pan Asia Wholesale Corporation (a shell corporation) for the sole purpose of entering into fictitious sales with Prestige Automobiles and then becoming an unauthorized reseller of vehicles to China.

12. In furtherance of the scheme, each vehicle that was sold through the above schemes on Guam, was subsequently registered in the fictitious buyer's name with the Guam Department of Motor Vehicles (DMV) as a bona fide sale when in fact no money had exchanged between buyer and seller, the buyer never took possession of the vehicle, and the documents being presented to the DMV represented false statements. These fictitious sales and false documentation were created by Shen Sr. and others so that the subsequent sale of the same vehicle in China would appear to be made by the fictitious buyers on Guam and not by Prestige

Automobiles who was prohibited to do so by the contractual agreements with BMW and Land Rover.

13. Vicky Acosta, Ocean Freight Manager, CTSI Logistics, Guam was interviewed by the FBI on August 22, 2016 and advised that all vehicles shipped to China by Pan Asia Wholesale Corporation were dropped off at CTSI Logistics by employees of Prestige Automobiles. CTSI packaged the vehicles for shipping to China in containers prior to their delivery to the Guam port for shipping.

14. Annie Nonesa, Office Assistant, Marianna Express Lines LTD (MELL), was interviewed by the FBI on August 22, 2016. Nonesa advised that Pan Asia Wholesale Corporation shipped new vehicles to China through MELL. Nonesa worked with Prestige Automobiles employee Ana Absalon to create required shipping documents for the vehicles being shipped to China by Pan Asia Wholesale Corporation. Absalon represented herself to Nonesa as acting on behalf of Pan Asia Wholesale Corporation for the shipping transactions. Marine insurance obtained by Pan Asia Wholesale Corporation for the vehicles being shipped to China was paid for by Absalon using a Prestige Automobiles credit card.

15. In order to conceal the proceeds from the China sales, Shen Sr. and others caused the sale proceeds to be laundered through an MGT Corporation account at First Hawaiian Bank (FHB) on Guam. A sum of $5,575,309.75 was wired into MGT Corporation's FHB account #02-042665 and $5,374,605.75 was paid out of the same account and deposited into Shen's Corporation and/or Prestige Automobiles (FHB account #03-061248) or Shen's Enterprises Co. dba Proline (FHB account #02-027747), via check. Bank account records for each of the above

accounts were received via subpoena and subsequently reviewed by the FBI, confirming the transactions.

16. In December 2017, Absalon, who has entered a guilty plea with the court and is cooperating with this investigation, reported that in late 2013 Shen Sr. directed her to create an alias email account in an attempt to conceal communications between Prestige Automobiles and the Chinese automobile broker(s). Absalon believed that she created kristina.santos@gmail.com or kristinasantos@gmail.com, Absalon could not recall exactly which, and Shen Sr. created davecabrera@gmail.com to communicate with the Chinese automobile broker(s).

17. Based on the above reporting I submitted an affidavit and application for search warrant before the Court for kristina.santos@gmail.com, kristinasantos@gmail.com and davecabrera@gmail.com. The search warrant was signed by the Court on January 4, 2018, and served on Google Inc. on January 5, 2018. Google Inc. subsequently returned results that were not relevant to Prestige Automobiles or the case at hand.

18. On February 20, 2018, Absalon was able to reset her password for an old Gmail account and confirmed through the account that the alias email account she created at the direction of Shen Sr. was, in fact, kristina.santos888@gmail.com. With consent from Absalon, I accessed kristina.santos888@gmail.com and created a download of the account. A review of the email account revealed more than 400 emails, between the timeframes of October 2013 and November 2015, containing discussions between Absalon, Shen Sr. and the Chinese automobile broker(s)'s email addresses (hxhauto@gmail.com and hy_0411@hotmail.com) regarding the types of vehicles being sent to China, the prices of the vehicles, the amount and timing of wires sent to pay for the vehicles, and names needed to register vehicles on Guam. Additionally, I

learned that Shen Sr. used the alias email account davecabrera269@gmail.com to communicate with Absalon's alias email account and the Chinese automobile broker(s).

19. I conclude that Shen Sr., Absalon, and other persons as yet unknown, created and used alias email accounts kristina.santos888@gmail.com and davecabrera269@gmail.com to facilitate a fraud scheme in violation of Title 18, United States Code, Section 371 (Conspiracy) Title 18, United States Code, Section 1343 (Wire Fraud), Title 18, United States Code, Section 1956(h) and 1957 (Money Laundering). Furthermore, I believe there is probable cause to suggest evidence of the above interactions and transactions, communications and details regarding transactions yet unknown, as well as the identities of additional individuals directly involved in the illegal activities, will be disclosed in email communications within davecabrera269@gmail.com

BACKGROUND CONCERNING EMAIL

20. In general, an email that is sent to Google, Inc., hereto after referred to as Google, subscriber is stored in the subscriber's "mail box" on Google servers until the subscriber deletes the email. If the subscriber does not delete the message, the message can remain on gmail.com servers indefinitely. Even if the subscriber deletes the email, it may continue to be available on Google servers for a certain period of time.

21. In my training and experience, I have learned that Google provides a variety of on-line services, including electronic mail (email) access, to the public. Google allows subscribers to obtain email accounts at the domain name gmail.com, like the email account listed in Attachment A. Subscribers obtain an account by registering with Google. During the registration process, Google asks subscribers to provide basic personal information. Therefore, the computers of Google are likely to contain stored electronic communications (including retrieved and un-

retrieved email for Google subscribers) and information concerning subscribers and their use of Google services, such as account access information, email transaction information, and account application information. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

22. A Google subscriber can also store with the provider files in addition to emails, such as address books, contact or buddy lists, calendar data, pictures (other than ones attached to emails), and other files, on servers maintained and/or owned by Google. In my training and experience, evidence of who was using an email account may be found in address books, contact or buddy lists, emails in the account, and attachments to emails, including pictures and files.

23. In my training and experience, email providers generally ask their subscribers to provide certain personal identifying information when registering for an email account. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. Based on my training and my experience, I know that even if subscribers insert false information to conceal their identity, this information often provides clues to their identity, location or illicit activities.

24. In my training and experience, email providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including

whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, email providers often have records of the Internet Protocol address (IP address) used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the email account.

25. In my training and experience, in some cases, email account users will communicate directly with an email service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Email providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

26. As explained herein, information stored in connection with an email account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored in connection with an email account can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, email communications, contacts lists, and images sent (and the data associated with the foregoing, such as date and time) may

indicate who used or controlled the account at a relevant time. Further, information maintained by the email provider can show how and when the account was accessed or used. For example, as described below, email providers typically log the Internet Protocol (IP) addresses from which users access the email account along with the time and date. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the email account access and use relating to the crime under investigation. This geographic and timeline information may tend to either inculpate or exculpate the account owner. Additionally, information stored at the user's account may further indicate the geographic location of the account user at a particular time (e.g., location information integrated into an image or video sent via email). Last, stored electronic data may provide relevant insight into the email account owner's state of mind as it relates to the offense under investigation. For example, information in the email account may indicate the owner's motive and intent to commit a crime (e.g., communications relating to the crime), or consciousness of guilt (e.g., deleting communications in an effort to conceal them from law enforcement).

CONCLUSION

27. Based on the forgoing, I request the Court issue the proposed search warrant for the email account listed in attachment A for items listed in Attachment B. Because the warrant will be served on Google who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

REQUEST FOR SEALING

28. I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the

targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may give targets an opportunity to flee/continue flight from prosecution, destroy or tamper with evidence, change patterns of behavior, notify confederates, or otherwise seriously jeopardize the investigation.

REQUEST FOR AN ORDER TO DELAY NOTIFICATION

29. It is respectfully requested that this Court, pursuant to 18 U.S.C. § 2705, issue an order delaying notification required under 18 U.S.C. § 2703(b) for a period of ninety (90) days, because there is reason to believe that notification of the existence of the order concerning this search warrant would seriously jeopardize the ongoing investigation described in this affidavit.

REQUEST FOR A NON-DISCLOSURE ORDER

30. It is respectfully that this Court, pursuant to 18 U.S.C. § 2705(a)(A), issue a nondisclosure order to Google, Inc. for a period of ninety (90) days, because disclosure to any individual or entity in any matter related to this search warrant would seriously jeopardize the investigation now in progress.

Further Affiant Saith Not.

Joshua M. Kipp
Special Agent
Federal Bureau of Investigation

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with davecabrera269@gmail.com, which is stored at premises controlled by Google, a company that accepts service of legal process at Google, Inc., c/o Custodian of Records, 1600 Amphitheater Parkway, Mountain View, California 94043.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Google, Inc., (the "Provider")

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Provider is required to disclose the following information to the government for the account listed in Attachment A from October 1, 2013 to November 30, 2015:

a. The contents of all emails associated with the account, including stored or preserved copies of emails sent to and from the account, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;

b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

c. The types of service utilized;

d. All records or other information stored at any time by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files;

e. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken.